CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS

OFFICE OF Privacy Protection

Activities of the Office of Privacy Protection

July 2001 – December 2002

BLANK

Message from the Chief

With the opening of the Office of Privacy Protection in 2001, California became the first state in the nation to have an agency dedicated to protecting individual privacy rights. I am proud of our state's leadership role in this important public policy area, and I am pleased with what the Office has been able to accomplish in its first year.

The Office of Privacy Protection gives Californians a place to go for help with their privacy problems and concerns. It also serves as a window on the marketplace, allowing us to learn what kinds of privacy problems people are experiencing, what practices organizations are employing to protect personal information, and how our privacy laws are working.

In this report, we share information on what we have done and what we have learned in the past year on the privacy beat in California. From the 1,700 people who attended the 26 educational workshops we conducted and the 3,600 who called or emailed us, we learned that identity theft is the number one privacy concern, followed by unwanted commercial solicitations. From law enforcement officials and business, we learned that education and guidelines are needed to make some of our new privacy laws work. Our consumer information sheets on identity theft, the process and forms for law enforcement to use in implementing a new identity theft law, and our "best practices" guidelines on protecting Social Security numbers are among the programs we developed to address these concerns.

My staff and I are committed to helping consumers and organizations, continuing to learn more about the evolving issue of privacy, and sharing our knowledge with the public and policy makers. We pledge to do our part to keep California at the forefront of privacy protection.

Joanne McNabb, Chief
Office of Privacy Protection
California Department of Consumer Affairs

BLANK

Contents

Overview 1

Consumer Assistance 3

Education and Information 6

Coordination with Law Enforcement 8

Recommended Policies and Practices 10

Plans for the Future 13

Appendix A: Advisory Council Members 15

Appendix B: Consumer Information Sheets 17

Appendix C: Recommendations on Social Security Numbers 41

Appendix D: Selected News Clips 57

BLANK

Overview

The establishment of California's Office of Privacy Protection, in the Department of Consumer Affairs, in 2001 coincided with a period of growing concern for individual privacy rights. Increasing awareness of the crime of identity theft, concern about finding a proper balance between privacy and security, and debates on the commercial use of personal information have spotlighted the challenges we face today in fulfilling the state Constitution's guarantee of an inalienable right of privacy.[1]

When the *Privacy Journal* in October 2002 named California as the leading state in the nation in protecting its citizens against invasions of privacy, it cited the creation of the Office of Privacy Protection as one of the factors that earned the state its top ranking.[2] California is one of only three states to have an office concerned with privacy and the only one whose office has a broad mandate to protect individual privacy.[3]

The mission of the Office of Privacy Protection, as defined in the legislation signed into law by Governor Gray Davis in 2000, is "protecting the privacy of individuals' personal information in a manner consistent with the California Constitution." The Office is to do this "by identifying consumer problems in the privacy area and facilitating [the] development of information practices in adherence with the Information Practices Act of 1977."[4]

The Office received funding in the 2001-2002 fiscal year, and the first months were devoted to hiring and training staff, setting up the physical office in the Department of Consumer Affairs, developing internal procedures, and producing informational materials. By November, the Office's web site was installed, containing consumer information sheets, major state and federal privacy laws, and links to other privacy resources. Office staff were responding to telephone calls and email from individuals with privacy problems and questions almost immediately. The Office announced its official opening on November 2, 2001, in Oakland, and on November 6, in San Diego.

The Office's enabling statute lays out four specific areas of responsibility:

- assisting consumers with identity theft and other privacy-related problems,
- providing information and education on privacy issues,
- working with law enforcement on investigations of identity theft and other privacy-related crimes, and

[1]Article 1, Section 1 of the California Constitution: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

[2]Privacy Journal, October 2002, Volume 28, Number 12. The full report on state rankings is available at http://www.privacyjournal.net/advocacy.htm.

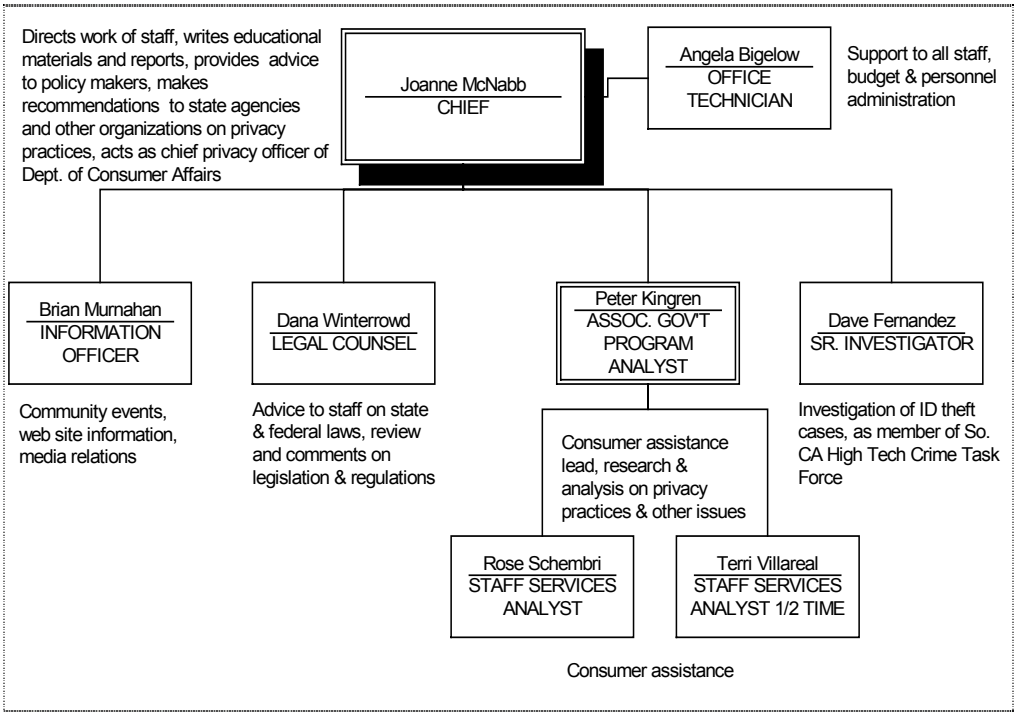
[3]The other two states are Hawaii and Minnesota. Their statutory scope is more limited than California's. Hawaii's Office of Information Practices is charged with administering the state's public records law, and Minnesota's Information Policy Analysis Division in the Department of Administration administers a government data practices act.

[4]SB 129 (Peace) of 2000 was enacted as California Business and Professions Code Section 350-352.

- recommending policies and practices that protect individual privacy rights.[5]

The Office has a small staff of 7.5 to perform these functions.

Figure 1: Office of Privacy Protection Organization Chart



The Office has relied on advice from many sources in developing its programs and policies. An ad-hoc advisory group of business and consumer representatives provided valuable perspectives when the Office was drafting its first major recommended practices document in May 2002. (See page 11 for more on this.) The Office created a standing Advisory Council in October 2002. The 15-member Council is comprised of a majority of consumer members (from privacy, consumer, civil rights, law enforcement and academic organizations), and seven representatives of industries with a particular interest in privacy issues (banking, insurance, retail, online and consumer information businesses).[6] The Advisory Council meets three times a year to provide advice and assistance on the Office's general plans and specific programs.

This report will describe the Office's activities in its first 14 months of operation in each of the four areas of responsibility and will end by highlighting plans for the future. (It should be noted that although the period from July 2001 through December 2002 covers 18 months, the Office did not officially open for business until November 2001, after the budget had passed, staff were hired, and basic operational systems were put in place.)

[5]California Business and Professions Code Sections 350(b), 350(c) and 350(e).

[6] See list of members of Advisory Council attached as Appendix A.

Consumer Assistance

Providing much-needed assistance and intervention services to consumers is one of the primary functions of the Office of Privacy Protection. Not only do Office staff help people with identity theft and other concerns, but we also learn from the people who contact us about what is happening in the marketplace, how current laws are working to address problems, and what new laws and other strategies might be needed to protect consumers from abuse.

From the official opening for business in November 2001 through December 2002, the Office of Privacy Protection was contacted by 3,600 people, who asked for assistance with privacy problems or concerns. Our consumer assistance philosophy is to empower consumers to help themselves by providing them with specific information, guidance, and, where appropriate, referrals. We refer a consumer to another agency only when we know that the agency can and will do something to help. If a consumer is in a particularly difficult situation, such as being unsuccessful after serious efforts or having limited abilities due to illness or age, we will intervene on the consumer's behalf. In such cases, we contact agencies and companies as necessary to help resolve the problems. We do not give legal advice, although we do provide information on state and federal privacy laws. We also contact businesses to let them know about consumer concerns about their information-handling practices, even when law does not address those practices.

Why People Contact the Office of Privacy Protection

More than half of those who contacted us in the past 14 months, whether on our toll-free telephone line or by email, did so about identity theft. (See Figure 2 on next page.) Forty-four percent told us they were victims of identity theft and 19% were concerned about how to avoid becoming victims. Victims who contacted us were in various stages: some had just received a call from a creditor or debt collector about a debt that wasn't theirs, others had been dealing with the results for some time and were having problems with a particular creditor or a credit bureau. Some had been arrested for unpaid traffic tickets or other crimes committed in their name by an imposter.

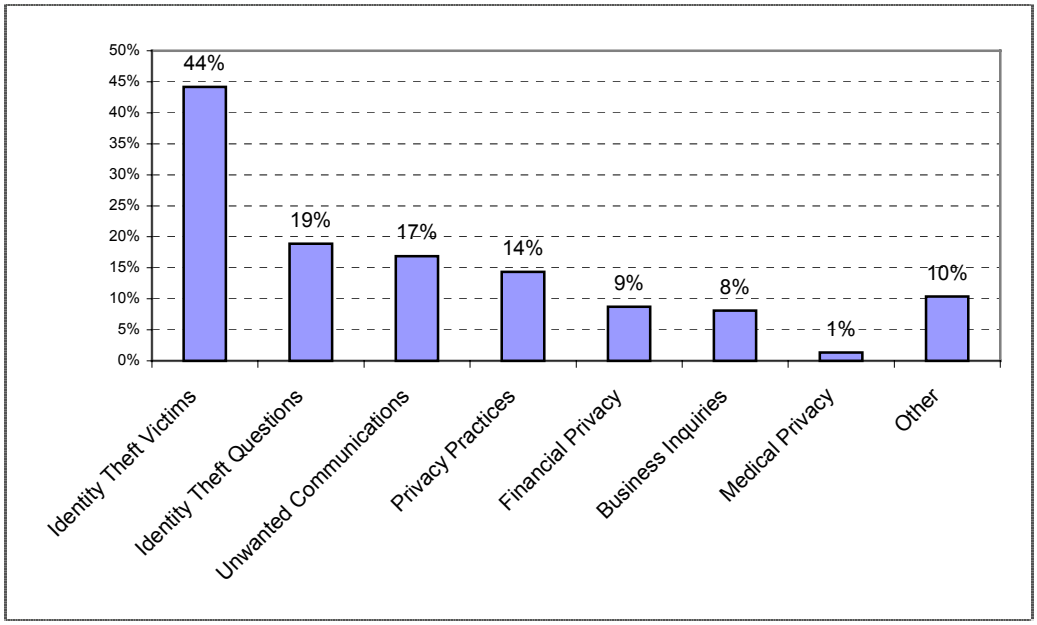
Complaints about unwanted solicitations ranked second, making up 17% of contacts to the Office. Nine percent were complaints about telemarketing calls, and 8% were complaints about junk mail, faxes or spam (unsolicited email advertisements).

Fourteen percent of contacts concerned the privacy practices of businesses or government. Many people said they objected strongly to giving their Social Security number to a business and asked if it was legal for a business to request the number. (It is. We advise them to ask questions, suggest alternatives, and if they're dissatisfied, to consider going to another company.) Others complained about businesses asking for other kinds of personal information, such as birth date, mother's maiden name, or telephone number, or wanted to know what additional personal information can be required when paying by credit card or by check. Some were unhappy about a business sharing their information with others.

Financial privacy concerns were the subject of 9% of contacts, primarily questions about how to read the privacy notices mandated by federal law or how to deal with debt collectors. Inquiries from businesses made up 8% of contacts. Many of these were requests for information on new state laws, most frequently on the new limitations on Social Security numbers or on the new laws on employee background checks.

Ten percent of the contacts are classified as "other." This category includes questions about the Office of Privacy Protection and non-privacy-related concerns.

Figure 2: Reasons People Contacted the Office of Privacy Protection, 11/ 2001 – 12/2002



Note: The total is more than 100%, because some contacts concerned more than one topic. This breakdown does not include the contacts about the Teale Data Center security incident in the spring and summer of 2002.

Highlight: Responding to a Security Breach

When a hacker compromised a server at the Teale Data Center containing a database of personal information on over 275,000 State employees in the spring of 2002, Governor Gray Davis called on the Office of Privacy Protection to provide information and assistance to employees. The Office did this in a variety of ways, including providing web site information, direct mail, individual assistance by phone and email, and employee workshops.

Information was immediately posted on the Office's web site, which was linked to the State Portal. A dedicated web page for State employees contained details on preventive measures to take for protection from the possibility of identity theft. The page also contained sample letters to credit bureaus, links to fact sheets, and frequently asked questions. A fact sheet with the same basic information was mailed to the homes of all affected employees. The Office made special arrangements with the credit reporting agencies to set up dedicated phone numbers with customized information for

State employees. The Office assisted more than 1,100 State employees who called or emailed in June and July of 2002. Office staff conducted seven workshops for State employees in the Sacramento area and produced a video version of the workshop, which was mailed to offices in other parts of the state.

The good news is that as of December 2002, law enforcement and credit reporting agencies report that they have found no evidence of identity theft having occurred as the result of this incident. An additional positive outcome of the event is the passage of the first law in the country requiring notification of security breaches.[7]

[7]Civil Code Sections 1798.29 and 1798.92, which take effect July 1, 2003, require private companies and state agencies to notify individuals if certain personal information is acquired by unauthorized persons. The information that triggers the notice is the kind that could subject someone to the risk of identity theft: name plus Social Security number, drivers license number, or financial account number.

Education and Information

The burden of protecting individual privacy falls largely on individuals, which makes the role of consumer education and information critical. The Office of Privacy Protection's first efforts were devoted to setting up an Internet web site containing consumer information on privacy topics, federal and California privacy laws, and a variety of information from and links to other privacy-related sites. While other privacy sites, such as those of the Privacy Rights Clearinghouse, the Identity Theft Resource Center and the Federal Trade Commission,[8] contain excellent information on privacy topics, the Office's goal was to produce basic consumer materials that are accessible and easy to read. Consumer information sheets are written generally at an eighth-grade reading level and are produced in English, Spanish, Chinese, Vietnamese, and Korean.[9]

The first topic we addressed is the most visible privacy problem of our time, and the fastest-growing crime—identity theft. Our "Identity Theft Prevention Tips" information sheet lists things consumers can do to lower their risk of becoming victims. Our "Identity Theft Victim Checklist" gives a step-by-step explanation of what victims of the various kinds of identity theft should do to clear up their situations.

The other two consumer information sheets we produced in this first year were on financial privacy and on protecting Social Security numbers. "Your Financial Privacy" explains how to take advantage of the rights provided in federal law to control personal financial information. "Your Social Security Number: Controlling the Key to Identity Theft" explains the consumer rights in the California law passed in 2001 that bars companies from publicly posting or displaying Social Security numbers and offers other tips for protecting Social Security numbers.

In order to reach the considerable portion of the population that does not have easy access to the Internet, we conducted 26 educational workshops in various parts of the state, each attended by an average of 65 people. Half of the workshops were conducted at the request of legislators at town hall meetings in their districts.[10] The workshops received local news coverage, thus increasing awareness off the Office as a resource for consumers. Workshops were conducted in Altadena, Bakersfield, Carmichael, Citrus Heights, Elverta, Folsom, Fresno, Laguna Woods, Sacramento, San Diego, San Leandro, San Rafael, Santa Rosa, and Vallejo.

In addition, we made shorter presentations at 22 community events and at 16 business, law enforcement and privacy organization conferences, and we distributed informational materials at four large consumer events.

---

[8] The Privacy Rights Clearinghouse is a small non-profit organization based in San Diego whose web site at www.privacyrights.org has a wealth of fact sheets, articles, and other information on a broad range of privacy topics. The Identity Theft Resource Center, a subsidiary of the Privacy Rights Clearinghouse, has in-depth information on identity theft at www.idtheftcenter.org. The FTC has a site dedicated to identity theft at www.consumer.gov/idtheft.

[9] The Office of Privacy Protection's Consumer Information Sheets are attached as Appendix B.

[10] Thirteen legislative workshops were held in response to invitations from Senators Ackerman, Alpert, Chesbro and Torlakson, and from Assembly members Cox, Figueroa, Kehoe and Wayne.

Highlight: Train the Trainers

In July, on the invitation of Senator Dick Ackerman, we conducted a workshop on identity theft for over 200 residents of the Orange County city of Laguna Woods. Laguna Woods is an unusual city, one of California's newest and oldest cities. Incorporated in 1999, the city's residents have an average age of 78. Ninety percent of the city's four square miles is contained within the gated senior citizen community of Leisure World. The balance of the city contains three additional senior residential communities and several thriving commercial centers.

After the July workshop a city councilman asked if the Office could train a group of residents so that they could help their neighbors take basic precautions against identity theft and also help any who should become victims with the necessary steps to clear up their situation. We developed a "train-the-trainers" manual on identity theft prevention and "first-aid" for victims. In October, we returned to Laguna Woods and trained the members of the Community Services Committee and provided them with the manual and with informational materials to give to their neighbors.[11] Office staff continues to provide advice and consultation to Committee members, and we plan to do a follow-up training session for them in 2003.

This train-the-trainers approach can allow the Office to serve more Californians and we plan to continue to provide similar training to community organizations in other parts of the state. This kind of outreach strategy enables us to maximize the Office's limited resources, which is particularly important in a difficult fiscal environment.

[11] See *Orange County Register* article in Appendix D.

Coordination with Law Enforcement

California's identity theft laws are among the most comprehensive in the nation, yet law enforcement reports that the incidence of the crime continues to grow here as elsewhere. The low-risk, high-reward crime, which commonly crosses jurisdictional lines, can be very difficult to investigate and prosecute. A multi-jurisdictional approach is being taken by five regional high-tech crime task forces, made up of representatives of local, state and federal law enforcement agencies.[12] In recent years these task forces have received state funds to be used for the investigation of identity theft. The Office of Privacy Protection assigned its Senior Investigator to serve on the Identity Theft Detail of the Southern California Task Force, which handled more than 5,000 cases of identity theft in 2002.[13]

Early in 2002, the Office contacted all the regional Task Forces, as well as all sheriff's offices and police departments, to let them know that they could refer identity theft victims to the Office for assistance in clearing up their records, thus freeing up law enforcement officials to investigate as many cases as possible.

The Chief of the Office of Privacy Protection served as a member of the Department of Motor Vehicles' Anti-Fraud Task Force. This group, which consisted primarily of law enforcement officials from all levels of government, was invited by the Director of Motor Vehicles to assist him in improving the DMV's programs to address fraud. The Task Force met for over a year and ultimately made a number of recommendations. The DMV has already adopted several of these, including some designed to help prevent identity theft by doing a better job of verifying the identity of applicants for licenses, vehicle registration, and official identification cards.

Highlight: Making a New Law Work

A law that took effect January 1, 2002 gave identity theft victims and law enforcement officials an important new tool.[14] Penal Code section 530.8, and related Financial Code and Civil Code sections, requires credit issuers and utilities to give an identity theft victim, or the victim's designated law enforcement representative, a copy of the application and other documents filed in connection with a fraudulently opened account. The victim must have a police report of identity theft. Getting access to these documents early in an investigation can be critical to identifying and arresting the thief. Early in 2002, however, many law enforcement officers were finding that credit issuers were unaware of the new law and were still requiring a search warrant before releasing the documents.

[12] The task forces are the Southern California High-Tech Crime Task Force in Los Angeles County, the Sacramento Valley Hi-Tech Crimes Task Force in Sacramento, North Bay HEAT in Napa, the REACT Task Force in Santa Clara County, and the CATCH Team in San Diego.

[13] The ID Theft Detail reports having served 147 search warrants, made 57 felony arrests and 6 misdemeanor arrests, and gotten 51 convictions in cases involving $686,000 in loss and $832,000 in property value recovered.

[14] Senate Bill 125 (Alpert), Chapter 493 of the Statutes of 2001.

When approached with this problem by two investigators, the Office of Privacy Protection worked with them and with Department of Justice staff to develop forms and a process to improve the implementation of the new law. The forms were sent with an explanatory letter to all local law enforcement offices and were also made available on a new Law Enforcement page on the Office's web site.

The process involves having local law enforcement officials refer cases where a creditor is not complying with the law to the Office. A call to the company's privacy officer or a letter from the Office usually results in compliance. When those efforts are unsuccessful, Office staff refers the matter to a Deputy Attorney General who works on identity theft for further action. Most of the reports of non-compliance involved cell phone companies, some of which were unclear on the law's application to them. A clarifying amendment to the Penal Code section was passed in 2002, to specifically identify cell phone companies as utilities subject to the law.[15]

[15] Senate Bill 1254 (Alpert), Chapter 254 of the Statutes of 2002.

Recommended Policies and Practices

In addition to providing individuals with assistance and information, the Office of Privacy Protection is directed to "make recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers."[16] This is one of the most important things the Office can do to influence organizations to adopt information-handling practices that protect individual privacy.

Many public and private organizations are seeing the need to revise their information-handling practices. They recognize that the proliferation of electronic databases of personal information and the use of the Internet to collect and transmit data create new risks to individual privacy. The increase in public concern about identity theft and hacking incidents are also contributing to the move to update organizational practices. While there are steps consumers can take to protect their personal information, it is the organizations that collect and maintain vast amounts of personal information on individuals that can have the biggest impact on reducing the incidence of identity theft.

Organizations are seeking guidance on "best practices" in handling personal information. As noted in a previous chapter, eight percent of the contacts to the Office were from representatives of businesses with questions on privacy laws and practices. Additionally, several of the new "privacy officers" that state agencies were required to designate by the same legislation that created the Office of Privacy Protection[17] contact the Office and ask for models of privacy practices and the role of privacy officers in encouraging good practices.

A set of model practices exists in the form of the Fair Information Practice Principles, first articulated by the U.S. Department of Health, Education and Welfare in 1973, and now widely accepted throughout the industrialized world.[18] These principles are the basis for many privacy laws in the United States, Canada, Europe, Australia, New Zealand, Hong Kong, and other parts of the world. For example, California's Information Practices Act of 1977, which applies to state agencies, is based on the principles. The basic principles are openness, collection limitation, purpose specification, use limitation, data quality, individual participation, security safeguards, and accountability.

In November 2002 a Senate committee hearing raised questions about the risk of identity theft created by the public record release of comprehensive indices of birth and death records. Several witnesses at the hearing pointed out that the records contained information such as mother's maiden name and Social Security number and the release of the entire state indices put that sensitive information into public circulation, such as on genealogy web sites. Governor Davis issued an Executive Order in December,

[16] California Business and Professions Code section 350(c).

[17] Government Code section 11019.9, which took effect in 2001, requires every state agency to enact and issue a privacy policy and to designate a position as responsible for the privacy policy. Civil Code section 1798.22 also requires state agencies to designate an employee as responsible for compliance with the requirements of the Information Practices Act.

[18] The principles are most recently formulated in the Organisation for Economic Cooperation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at http://www1.oecd.org/publications/e-book/9302011E.PDF.

directing the Department of Health Services, whose Center for Health Statistics maintains the birth and death record indices, to stop releasing them and to review the conditions under which the indices should be released to the public. The Office of Privacy Protection provided recommendations to the Department of Health Services on how to achieve an appropriate balance between the privacy interests of individuals and the public's interest in open government. An Administration-sponsored bill passed in 2002 resulted in a new law that removes the mother's maiden name and Social Security number, the information that puts individuals at risk of identity theft, from the publicly available versions of the indices.[19]

Courts are among the organizations currently working on updating their information-handling practices to take into account changes in the way personal information is collected and stored. In April of 2002, the Office of Privacy Protection made recommendations in the form of comments on a draft Model Policy on Public Access to Court Records published by the National Center for State Courts and the Justice Management Institute.[20] The model policy was drafted to provide guidelines to state courts to help them achieve a balance between ensuring privacy and providing public access to court records.

Highlight: Social Security Number Guidelines

In the fall of 2001, Governor Davis signed a landmark privacy law prohibiting private-sector organizations from publicly posting or displaying Social Security numbers.[21] The law is the first in the nation aimed at preventing the abuse of Social Security numbers, which have come to play a major role in the marketplace and in identity theft. Soon thereafter the Office of Privacy Protection began to receive calls and emails from businesses asking what agency would be issuing regulations or guidelines for the new law. We explained that while there is no regulatory agency for the law the Office intended to publish recommended practices for protecting Social Security numbers. Shortly before the July 1, 2003 first-phase implementation date of the new law, the Office published its *Recommended Practices for Protecting the Confidentiality of Social Security Numbers*.[22]

In developing the recommendations, the Office of Privacy Protection received consultation and advice from a 14-member advisory committee made up of representatives of the financial, insurance, health care, retail and information industries, and of consumer privacy advocates. The Office also relied on the Fair Information Practice Principles. The resulting recommended practices address the issues in the California law and also go beyond it to cover internal practices. The recommended practices are appropriate for the private and public sectors, even though the law does

---

[19] Senate Bill 1614 (Speier) of 2002 enacted Health & Safety Code Sections 102231 and 102232, and amended Section 102230, effective January 1, 2003.

[20] The draft and final versions of the model policy, along with a summary of the comments received, are available at www.courtaccess.org/modelpolicy/. The comments of the Office of Privacy Protection are available at www.privacy.ca.gov/recommendations/courtrecords.pdf.

[21] Civil Code section 1798.85, enacted by Senate Bill 168 (Bowen) in 2001, and amended by Assembly Bill 1068 (Wright) and Senate Bill 1730 (Bowen) in 2002.

[22] Attached as Appendix C.

not apply to government, and they could be followed for handling other kinds of sensitive personal information in addition to Social Security numbers.

Plans for the Future

The Office of Privacy Protection has gotten off to a good start. In its first 13 months of operation, the Office assisted over 3,600 people with identity theft and other privacy concerns, and provided consumers with information and education at 26 educational workshops, 38 community and organizational events, and four large consumer fairs. The Office initiated a productive working relationship with local law enforcement, including dedicating a staff member to one of the regional identity theft task forces and developing materials to assist law enforcement in the implementation of a new identity theft law. The Office began work in the important area of organizational practices by publishing a set of recommendations on handling Social Security numbers, the critical item of personal information that has come to create a major risk of identity theft.

Fiscal Year 2002-2003

This report covers activities for the first half of the 2002-2003 fiscal year. Additional programs are underway or planned for the second half of the year.

- *Consumer Information Sheets*

  New consumer information sheets on how to control unwanted marketing communications (telemarketing, junk mail, junk faxes, spam), health privacy, and consumer background checks.

- *Consumer Information for Criminal Identity Theft Victims*

  Self-help materials for victims of criminal identity theft. Such victims can suffer repeated arrests for a crime committed by someone else using the victim's identity. While current law provides some relief for criminal identity theft victims (in the form of a database in the Department of Justice and expedited court proceedings), practical problems have prevented many victims from taking advantage of these resources. The Office's materials will enable such victims to obtain the mandatory court order that will qualify them for inclusion in the DOJ database—without having to incur large attorney fee obligations. Students at Stanford's Center for Internet and Society Cyber Law Clinic currently assist the Office on this project.

- *Privacy Practice Recommendations for State Agencies*

  Information-handling practice recommendations for State agencies, intended to help agencies comply with the Information Practices Act in the era of e-government. The first stage of that project is a review and revision of the practices of the Department of Consumer Affairs, as a pilot for other agencies.

- *Privacy Practice Recommendations on Consumer Background Checks*

  Recommended practices for conducting consumer background checks, in follow-up to recent legislation that amended the Investigative Consumer Reporting Agencies

Act to increase protection for identity theft victims.[23] The Office's recommendations will be intended to provide guidance to business, and particularly to small businesses and landlords, in the responsible use of consumer information services in conducting background checks of prospective employees and tenants. An ad-hoc advisory group of interested industry and consumer representatives will assist in the development of the recommendations.

- *Uniting Privacy and the First Amendment in the 21st Century*

  In May 2003, the Office will sponsor, along with the First Amendment Project and the Electronic Privacy Information Center, a public forum, Uniting Privacy and the First Amendment in the 21st Century. The forum will take place in Oakland on May 9-10. One of the topics that will be addressed at the forum is one of the most significant public policy issues Americans face today: the balancing of the competing values of public access to government records with individual privacy rights.

Fiscal Year 2003-2004

The dire budget situation will make the 2003-2004 fiscal year a challenge for the Office of Privacy Protection. Even with significant reductions in its small budget, the Office will continue to provide the public with information and assistance on privacy rights. The Office will provide information primarily through its Internet web site and "free" publicity, along with a few educational workshops and community meetings. Individuals will continue to receive assistance with identity theft victim and other privacy concerns via email and the toll-free telephone line, although a reduction in staffing would mean that somewhat less service would be available. Some work on privacy practices, primarily State agency practices, will also continue.

[23] The California Investigative Reporting Agencies Act, Civil Code Sections 1786-1786.60, was amended by Assembly Bill 655 (Wright) of 2001, and by Assembly Bill 1068 (Wright) and Assembly Bill 2068 (Wright) of 2002.

Appendix A: Office of Privacy Protection Advisory Council Members

Brent Barnhart
Senior Counsel
Kaiser Foundation Health Plan Inc.

James Clark
Vice President, Government Relations
California Bankers Association

Anne Eowan
Vice President
Association of California Life and Health Insurance Companies

Jay Foley
Director of Consumer and Victim Services
Identity Theft Resource Center

Mari Frank
Attorney, Privacy Consultant, Author

Beth Givens
Director
Privacy Rights Clearinghouse

Richard Holober
Executive Director
Consumer Federation of California

Chris Larsen
Chairman and CEO
E-LOAN

Deirdre Mulligan
Director
Samuelson Law, Technology & Public Policy Clinic
Boalt Hall School of Law
University of California, Berkeley

Daniel Nestel
Director, State Government Affairs
Reed Elsevier Inc.

Dr. Peter G. Neumann
Principal Scientist
Computer Science Lab
SRI International

Wendy Schmidt
OVP, Assistant General Counsel
Federated Department Stores, Inc.

Sam Sorich
Vice President and Western Regional Manager
National Association of Independent Insurers

Lee Tien
Senior Staff Attorney
Electronic Frontier foundation

Lt. Mike Tsuchida
Sacramento Valley Hi-Tech Crime Task Force

BLANK

Appendix B: Consumer Information Sheets

BLANK

OFFICE OF Privacy Protection

Identity Theft Prevention Tips

CONSUMER INFORMATION SHEET 1

An identity thief takes some piece of your personal information and uses it without your knowledge. The thief may run up debts or even commit crimes in your name. It may not be possible to completely prevent identity theft. But you can lower your risk of becoming a victim.

♦ Protect yourself.

Manage your personal information wisely. Protect your home address, home telephone number, Social Security number, bank and credit card account numbers, and PIN numbers.

♦ Don't carry your Social Security card in your wallet.

It's an open invitation for an identity thief. Check your health plan and other cards. They may have your Social Security number on them. Carry only the identifying information that you need.

♦ Tear up or shred papers.

Tear up or shred papers with personal information before you throw them away. Tear up credit card offers and "convenience checks" that you don't use.

♦ Don't give out personal information on the phone.

Don't give out your personal information on the phone – unless you made the call or know the caller. The same goes for mail. Any personal information you put on the Internet may be especially vulnerable.

♦ Ask how your information will be used.

Before you give any personal information to a business, ask how it will be used. Ask if the business will share your information with others. Ask if you can have your personal information kept confidential.

♦ Control your financial information.

If you want to limit the sharing of your financial information, write to your bank, and your credit card, insurance, and securities companies. Tell them that you want to "opt-out" of sharing your personal financial information with outside companies. You are permitted to do this under federal

law.[1] See "Your Financial Privacy (CIS3)" on our Financial Privacy web page.

♦ Check your bills.

Check your credit card bills carefully each month. Look for unauthorized charges and report any to your card issuer immediately. Call if bills don't arrive on time. It may mean that someone has changed the address or other information so that you would not learn about fraudulent charges.

♦ Get your name off marketing lists.

Stop pre-approved credit card offers. Have your name removed from credit bureau marketing lists. Call toll-free 888-5OPTOUT (888-567-8688).

Have your name, address, and phone number removed from many other marketing lists. Contact the Direct Marketing Association. This will not stop all marketing mailings and telephone calls, but it will cut out many.

DMA Mail Preference Service
P. O. Box 643
Carmel, NY 10512
Or online (for a $5 charge) at
www.the-dma.org

DMA Telephone Preference Service
P. O. Box 1559
Carmel, NY 10512
Or online (for a $5 charge) at
www.the-dma.org

Tell telemarketers who call you to put you on their "do not call" list. Federal law requires them to do this.[2]

♦ Check your credit reports.

Get copies of your credit reports from the three major credit bureaus at least once a year. Check for changed addresses or fraudulent account information. Copies cost about $8. To order your reports, contact:

Equifax	Experian	TransUnion
800-685-1111	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

[1] The Financial Services Modernization Act (or Gramm-Leach-Bliley Act), 15 U.S. Code 6801-6810.
[2] The Telephone Consumer Protection Act, 47 CFR 64.1200. The Telemarketing and Consumer Fraud Abuse Prevention Act, 16 CFR 310.

OFFICE OF Privacy Protection

Your Financial Privacy Rights

CONSUMER INFORMATIO N SHEET 2

Get control of your financial information.

Controlling your personal information is an important part of personal privacy. Personal financial information is among the most sensitive of all personal information. Personal financial information includes what you put on an application for a loan or credit card, your account balances, your payment history, your overdraft history, and where you make purchases by debit or credit card. In some instances, it can even include medical information.

New federal law gives new consumer rights.

A new federal law allows consumers to put some limits on what banks and other financial companies can do with your personal financial information. [1] The law applies to banks, credit unions, savings and loans, credit card companies, insurance companies and other financial service companies. [2]

You can say no.

The law lets you tell your bank and other financial companies that you do not want them to share your personal financial information with outside companies. You do not have the right to stop all sharing of your financial information, but you have some control. [3]

Notices sent to consumers.

The law requires the financial companies to notify their customers of their privacy rights every year. The first notices had to be sent by July 1, 2001. Many people did not notice these privacy notices. The notices were mixed in with other bill inserts. The notices were often written in legal language that was hard to understand. [4]

How to say no, or how to "opt-out."

Opt-out means that if you say "no" — that you don't want your personal financial information shared with outside companies — then the financial company must follow your wishes. But if you say nothing, if you do not opt-out, then the financial company is free to share your information with outside companies. [5]

You also have the right to opt-out of having some of your financial information shared with affiliated companies (companies in the same "family"). This opt-out right may be on the same notice, or may come later on a different notice.[6]

400 R Street, Suite 3080 • Sacramento, CA • 95814 • 1.866.785-9663
www.privacy.ca.gov • email: privacy@dca.ca.gov

It's not too late.

It's not too late to opt-out, even if you did not reply to the privacy notices in the time given (usually 30 days). If you didn't reply, then your financial company may have already started sharing your information with outside companies. But you have a continuing right to opt-out and you can prevent future sharing of more current information.

Follow the company's instructions.

The notices sent by your financial companies had to tell you how to opt-out. The notices probably gave you a choice of writing a letter, returning a form, calling a toll-free number or using the Internet. [6]

If you want to opt-out, you should follow your financial company's instructions. Even if you can opt-out by phone or over the Internet, it is still a good idea to write a letter to create a record of your action. Sample opt-out letters are available from the Privacy Rights Clearinghouse at www.privacyrights.org/fs/fs24a-letter.htm and from Junkbusters.com at www.junkbusters.com/optout.html. A list of the opt-out addresses and toll-free numbers of financial companies is also available from the Privacy Rights Clearinghouse at www.privacyrights.org/fs/fs24a-OptOutAddresses.htm.

You can ask for more privacy.

You can, of course, ask for more privacy protection than the law requires. For example, you could ask your financial company not to share your personal financial information with affiliates or with joint marketers. Even if your request is not honored, telling your financial companies that you care about your personal privacy may lead them to change their policies in the future.

What if you think your privacy rights were violated?

You can make a complaint to a government agency that regulates financial companies. The agency may investigate your complaint and may take action against the financial company. But the agency can't represent you. You have the right to sue under one of the federal laws, but not under the other law.[7]

Before filing a complaint or taking legal action, consider writing a letter to the financial company or the government agency. In your letter, explain why you think the company violated the law and what you would like it to do for you. Ask for a specific response within a reasonable time (for example, 30 days).

Financial Privacy Laws

Financial Services Modernization Act (GLB), 15 USC 6801-6810
www.ftc.gov/privacy/glbact/glbsub1.htm

Federal Trade Commission Final Rule on Privacy of Consumer Financial Information, 16 Code of Federal Regulations Part 313
www.ftc.gov/os/2000/05/65fr33645.pdf

Fair Credit Reporting Act (FCRA), 15 USC 1681-1681u
www.ftc.gov/bcp/conline/edcams/fcra/

Government Agencies

The following government agencies can enforce the privacy protections in the laws listed above.

Federal Trade Commission
Investigates consumer fraud outside the jurisdiction of other federal agencies.
FTC
Office of Consumer Protection
CRC-240
Washington, DC 20580
877-FTC-HELP (877-382-4357)
www.ftc.gov/privacy
email: consumerline@ftc.gov

Federal Reserve Board
Regulates banks other than national banks and branches of foreign banks.
Federal Reserve
Consumer & Community Affairs
20th & C Streets, NW Stop 801
Washington, D.C. 20551
202-452-3693
www.federalreserve.gov/pubs/complaints

Office of the Comptroller of the Currency
Regulates national banks and branches of foreign banks.
OCC
Customer Assistance Group
1301 McKinley St., Suite 3710
Houston, TX 77010
800-613-6743
www.occ.treas.gov/customer.htm
email: customerassistance@occ.treas.gov

Office of Thrift Supervision
Regulates federal savings associations and savings banks and state-chartered savings associations.
OTS
Consumer Complaints
1700 G Street, NW
Washington, DC 20552
202-906-6237
800-842-6929
http://www.ots.treas.gov/pagehtml.cfm?catNumber=35
email: consumer.complaint@ots.treas.gov

Securities and Exchange Commission
Oversees stock exchanges, broker-dealers and associates, and investment advisers.
SEC Complaint Center
Investor Education & Assistance
450 Fifth St., NW
Washington, DC 20549
202-942-7040
www.sec.gov/consumer/compform.htm

National Credit Union Administration
Regulates federal credit unions.
GLB & FCRA Address:
NCUA
Director, Division of Supervision
2300 Clayton Rd., Suite 1350
Concord, CA 94520
www.ncua.gov/talk2ncua/talk2ncua.html
email: region6@ncua.gov

California Department of Insurance
Regulates insurance industry in California.
Department of Insurance
Consumer Communications Bureau
300 So. Spring St.
Los Angeles, CA 90013
800-927-HELP
213-897-8921
email: 927HELP@insurance.ca.gov

Notes

[1] The Financial Services Modernization Act, or Gramm-Leach-Bliley Act, 15 U.S. Code 6801-6810. Known as the GLB Act, the law allows financial institutions, insurance and investment companies to merge, becoming what have been called one-stop financial supermarkets.

[2] The GLB Act considers a broad array of businesses to be "financial institutions," including, for example, retailers that issue their own credit cards directly to consumers, real estate appraisers, mortgage brokers, career counselors in the finance area, check printing businesses, and accountants who prepare tax returns.

[3] There are two exceptions to the consumer's opt-out right to prevent the sharing of their personal financial information with other companies under federal law. The exceptions are affiliates and joint marketing agreements. *Affiliate sharing*: The GLB Act allows financial institutions to share their customers' personally identifiable financial information with their affiliated companies—and some larger institutions have many affiliates in a variety of lines of business. The GLB Act does not give consumers the right to opt-out of that kind of information sharing. The other exception to consumer choice about information sharing under the GLB Act is *joint marketing agreements* to sell financial products or services. You have no opt-out right to prevent your bank, for example, from sharing your personally identifiable financial information with a non-affiliated company with which it has a joint marketing agreement to sell financial products or services. Your bank could have an agreement with a non-affiliated company to market investment advisory services or insurance services. With such a marketing agreement, your bank could share your information with the other company after giving you notice that it provides such information to companies that perform marketing services for it. The GLB Act offers some protection in that the marketing agreement must require the third party to maintain the confidentiality of the information.

[4] The privacy notices were required to include the following information: how the customer's personal financial information is collected, how the customer's information is used, and how the customer could "opt-out" or choose not to have personal financial information shared with some outside or "third-party" companies.

[5] An alternative to opt-out is **opt-in.** The GLB Act does not give consumers any opt-in rights. An opt-in system would put control of your personally identifiable financial information in your hands. Under opt-in, the financial institutions would have to get your permission *before* they can share your personal financial information.

[6] Another federal law, the Fair Credit Reporting Act (FCRA), gives consumers the right to opt-out of having a limited amount of their personally identifiable financial information shared with affiliated companies. The FCRA allows you to opt-out of having "creditworthiness" information shared with affiliates. This includes information such as your payment history (whether you pay on time or late), your credit score and other information from your credit report. Neither the GLB Act nor the FCRA allows consumers to stop a company from sharing the more sensitive "transaction and experience" information with affiliates. Transaction and experience information includes, for example, what you charge on your credit card.

[6] The notices probably allowed you to opt-out under both the GLB Act and the FCRA. You do not have to opt-out every year. Your financial institutions must continue to follow your opt-out decision until you change it.

[7] You can't go to court to sue the company under the GLB Act. Under the FCRA, you have the right to sue the credit reporting agency in federal or state court. You could recover damages from violators of the FCRA.

BLANK

Identity Theft Victim Checklist

CONSUMER INFORMATION SHEET 3

This checklist can help identity theft victims to clear up their records. It lists the actions most identity theft victims should take to limit the damage done by the thief. Use the contact logs at the end of the checklist to keep a record of all your contacts with credit bureaus, creditors and others. Keep copies of all the letters you send and receive.

For more information, see the web sites of the Federal Trade Commission (www.consumer.gov/idtheft), the Identity Theft Resource Center (www.idtheftcenter.org), the Privacy Rights Clearinghouse (www.privacyrights.org), and the Department of Consumer Affairs (www.dca.ca.gov).

✓ Report the fraud to the three major credit bureaus.

Ask each of the credit bureaus to flag your file with a "fraud alert." Also, ask them to add a victim's statement to your credit report. The victim's statement tells creditors to call you to get your approval if they receive requests to open new accounts. Give them a phone number to use to contact you. Ask each credit bureau for a free copy of your credit report. As a victim of identity theft, you have the right to a free report from each credit bureau. For more on what to tell the credit bureaus, see "Identity Theft: What to Do When It Happens to You" at www.privacyrights.org/fs/fs17a.htm.

✓ Report the crime to the police.

Under California law, you can report identity theft to your local police department. Ask the police to issue a police report of identity theft. You may have to show copies of the laws to the police. The laws are on the last pages of this information sheet. Give the police as much information on the theft as possible. Give them any new evidence you collect to add to your report. Be sure to get a copy of your police report. You will need to give copies to creditors and the credit bureaus. For more information, see "Organizing Your Identity Theft Case" by the Identity Theft Resource Center, available at www.privacyrights.org/fs/fs17b-org.htm.

✓ Request information on fraudulent accounts.

When you file your police report of identity theft, the officer may give you forms to use to request account information from credit grantors. If the officer does not do this, you can use the forms available from the Office of Privacy Protection at www.privacyprotection.ca.gov/howto530.8.htm. Send copies of the forms to all creditors where the thief opened or applied for accounts, along with copies of the police report as described below. Give the information you receive from creditors to the officer investigating your case.

✓ Call creditors.

Call all creditors for any accounts that the thief opened or used. When you call, ask for the security or fraud department. Creditors can be credit card companies, other lenders, phone companies, other utility companies, and department stores. Tell them you are an identity theft victim. Ask them not to hold you responsible for charges the thief made. Ask them to close those accounts and to report them to credit bureaus as "closed at consumer's request." If you open new accounts, have them set up to require a password or PIN to approve use. Don't use your mother's maiden name or the last four numbers of your Social Security number as your password. For more information on what to tell creditors, see the "Identity Theft: What to Do When It Happens to You," available at www.privacyrights.org/fs/fs17a.htm and the Federal Trade Commission's "When Bad Things Happen to Your Good Name," available at www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.

✓ Review your credit reports carefully.

Look for accounts opened in your name that you did not open. Also, look for charges to your accounts that you did not make. And look for late payments or non-payments that are not yours. Check your name, address and Social Security number. Look at the Inquiries section of the report. Ask the credit bureaus to remove any inquiries from companies holding fraudulent accounts in your name. Ask each credit bureau to remove all information in your credit report that results from the theft. Order new credit reports every three months until your situation has cleared up. You may have to pay $8 for each report after the first free one.

✓ Use the ID Theft Affidavit.

The Federal Trade Commission's ID Theft Affidavit is a form that can help you clear up your records. The Affidavit is accepted by the credit bureaus and by many major creditors. Send copies of the completed form to creditors where the thief opened accounts in your name. Also send copies to creditors where the thief made charges on your account, to the credit bureaus, and to the police. The form is available on the FTC web site at www.consumer.gov/idtheft/affidavit.htm.

✓ Write to the credit bureaus.

Write a letter to each credit bureau. Repeat what you said in your telephone call (see above). Send copies of your police report and completed ID Theft Affidavit. Remind the credit bureaus that they must remove any information that you, an identity theft victim, say is the result of the theft. Send your letters by certified mail, return receipt requested. Keep a copy of each letter.

✓ Write to creditors.

Write a letter to each creditor. Repeat what you said in your telephone call (see above). Send copies of your police report and the completed ID Theft Affidavit. Send your letters by certified mail, return receipt requested. Keep copies of your letters. Continue to review your bills carefully and report any new fraudulent charges to the creditor.

✓ If your checks or bank account information were stolen…

Close your bank account. Open a new one with a new account number. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Report the stolen checks to the check verification companies that stores use. For more information on stolen checks, see "Identity Theft: What to Do When It Happens to You," at www.privacyrights.org/fs/fs17a.htm.

✓ If your driver's license or DMV-issued ID card was stolen…

Immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license. Then call the toll-free DMV Fraud Hotline at 866-658-5758. If the thief is using your license as ID, you may want to change your license number. Ask DMV for an appointment. Take a copy of the police report and copies of bills or other items supporting your claim of fraud. You will also need to prove your identity. Take current documents such as a passport, a certification of citizenship or naturalization, or a U.S. military photo ID. DMV will issue a new driver's license or ID card number when you meet all the requirements. For more information, see "Identity Theft: Have You Been A Victim of Identity Theft? DMV Can Help," available at www.dmv.ca.gov/pubs/brochures/fast_facts/ffdl24.htm.

✓ If your mail was stolen or your address changed by the identity thief…

Notify the Postal Inspector if you think the identity thief has stolen your mail or filed a change of address request in your name. To find your nearest Postal Inspector, look in the white pages of the telephone book for the Post Office listing under United States Government. Or go to the Postal Inspection Service's web site at http://www.usps.com/ncsc/locators/find-is.html.

✓ If you are wrongly accused of a crime committed by the identity thief…

In the case of a false civil judgment, contact the court where the judgment was entered. Report that you are a victim of identity theft. In the case of a false criminal judgment, contact the California Department of Justice at 888-880-0240 and the FBI. Ask them for information on how to clear your name. To find the local field office of the FBI, look in the white pages of the telephone book for the FBI under United States Government. Or go to the FBI's web site at http://www.fbi.gov/contact/fo/fo.htm).

✓ If you are contacted by a debt collector…

Tell the debt collector that you are the victim of identity theft. Say that you dispute the validity of the debt. Say that you did not create the debt and are not responsible for it. Send the collector a follow-up letter saying the same things. Include a copy of your police report and of any documents you've received from the creditor. Write that your letter gives notice to a claimant under California Civil Code section 1798.93(c)(5) that a situation of identity theft exists. Send the letter by certified mail, return receipt requested.

If the debt collector is not the original creditor, send your letter within 30 days of receiving the collector's first written demand for payment.

✓ A word about your Social Security number ...

Sometimes, an identity thief will use the victim's Social Security number to be able to work. It's a good idea to check your Social Security earnings record to see if the thief is using your Social Security number. You can get a copy of your earnings record by calling 1-800-772-1213. Or get a Request for Social Security Statement (Form 7004) at www.ssa.gov/online/ssa.7004.pdf. If the thief is using your Social Security number, call the Social Security Fraud Hotline at 1-800-269-0271. You can also read "When Someone Misuses Your Number" at www.ssa.gov/pubs/10064.html.

Calls to Credit Bureaus

Credit Bureau	Date	Contact Person	Comments
Equifax 800-525-6285			
Experian 888-397-3742			
Trans Union 800-680-7289			

Calls to Police

Date	Contact Person	Comments

Calls to Creditors

Creditor	Date	Contact Person	Comments

Letters to Credit Bureaus

Credit Bureau	Date Sent
Equifax P. O. Box 740241 Atlanta, GA 30374	
Experian Consumer Fraud Assistance P. O. Box 949 Allen, TX 75013	
Trans Union Fraud Victim Assistance Division P. O. Box 6790 Fullerton, CA 92834	

Letters to Creditors

Creditor	Date Sent

Remember to send letters by certified mail, return receipt requested. Keep copies of all letters.

Calls to Check Verification Companies

Company	Phone Number	Date	Contact Person	Comments
CheckRite	800-766-2748			
Chexsystems	800-428-9623			
CrossCheck	800-843-0760			
Equifax	800-437-5120			
SCAN	800-262-7771			
Telecheck	800-710-9898			
International Check Services	800-526-5380			

Penal Code Section 530.5: Definition of Identity Theft

530.5 (a) Every person who willfully obtains personal identifying information, as defined in subdivision (b), of another person without the authorization of that person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, or medical information in the name of the other person without the consent of that person, is guilty of a public offense, and upon conviction therefor, shall be punished either by imprisonment in a county jail not to exceed one year, a fine not to exceed one thousand dollars ($1,000), or both that imprisonment and fine, or by imprisonment in the state prison, a fine not to exceed ten thousand dollars ($10,000), or both that imprisonment and fine.

(b) "Personal identifying information," as used in this section, means the name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit card number of an individual person.

(c) In any case in which a person willfully obtains personal identifying information of another person without the authorization of that person, and uses that information to commit a crime in addition to a violation of subdivision (a), and is convicted of that crime, the court records shall reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

Penal Code Section 530.6: Police Jurisdiction and Expedited Judicial Action

530.6 (a) A person who has learned or reasonably suspects that his or her personal identifying information has been unlawfully used by another, as described in subdivision (a) of Section 530.5, may initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction over his or her actual residence, which shall take a police report of the matter, provide the complainant with a copy of that report, and begin an investigation of the facts or, if the suspected crime was committed in a different jurisdiction, refer the matter to the law enforcement agency where the suspected crime was committed for an investigation of the facts.

(b) A person who reasonably believes that he or she is the victim of identity theft may petition a court for an expedited judicial determination of his or her factual innocence, where the perpetrator of the identity theft was arrested for or convicted of a crime under the victim's identity, or where the victim's identity has been mistakenly associated with a record of criminal conviction. Any judicial determination of factual innocence made pursuant to this section may be heard and determined upon declarations, affidavits, police reports, or other material, relevant, and reliable information submitted by the parties. Where the court determines that the petition is meritorious and that there is no reasonable cause to believe that the petitioner committed the offense for which the perpetrator of the identity theft was arrested or convicted, the court shall find the petitioner factually innocent of that offense. If the petitioner is found factually innocent, the court shall issue an order certifying this determination. The Judicial Council of California shall develop a form for use in issuing an order pursuant to these provisions. A court issuing a determination of factual innocence pursuant to this section may at any time vacate that determination if the petition, or any information submitted in support of the petition, is found to contain any material misrepresentation or fraud.

Penal Code Section 530.7: ID Theft Victim Data Base

530.7 (a) In order for a victim of identity theft to be included in the data base established pursuant to subdivision (c), he or she shall submit to the Department of Justice a court order obtained pursuant to any provision of law, a full set of fingerprints, and any other information prescribed by the department.

(b) Upon receiving information pursuant to subdivision (a), the Department of Justice shall verify the identity of the victim against any drivers license or other identification record maintained by the Department of Motor Vehicles.

(c) The Department of Justice shall establish and maintain a data base of individuals who have been victims of identity theft. The department shall provide a victim of identity theft or his or her authorized representative access to the data base in order to establish that the individual has been a victim of identity theft. Access to the data base shall be limited to criminal justice agencies, victims of identity theft, and individuals and agencies authorized by the victims.

(d) The Department of Justice shall establish and maintain a toll free number to provide access to information under subdivision (c). (e) This section shall be operative September 1, 2001.

Penal Code Section 530.8: Access to Information on Fraudulent Accounts

If a person discovers that an application in his or her name for a loan, credit line or account, credit card, charge card, or utility service has been filed with any person by an unauthorized person, or that an account in his or her name has been opened with a bank, trust company, savings association, credit union, or utility by an unauthorized person, then, upon presenting to the person or entity with which the application was filed or the account was opened a copy of a police report prepared pursuant to Section 530.6 and identifying information in the categories of information that the unauthorized person used to complete the application or to open the account, the person shall be entitled to receive information related to the loan, credit line or account, credit card, charge card, utility service, or account, including a copy of the unauthorized person's application or application information for, and a record of transactions or charges associated with, the loan, credit line or account, credit card, charge card, utility service, or account. Upon request by the person in whose name the application was filed or in whose name the account was opened, the person or entity with which the application was filed shall inform him or her of the categories of identifying information that the unauthorized person used to complete the application or to open the account.

OFFICE OF Privacy Protection

Your Social Security Number: Controlling the Key to Identity Theft

CONSUMER INFORMATION SHEET 4

⊡ Your Social Security number is the key.

Originally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information.

With your SSN, an identity thief can get your credit history, your bank account, your charge accounts, and your utility accounts. A thief can also use the number to open new credit and bank accounts or to get a driver's license—all using your identity.

⊡ Don't carry your Social Security card in your wallet.

You don't need to have your Social Security card with you at all times. Keep it at home in a safe place. Check for other cards that may have your SSN on them.

⊡ Ask questions when they ask for your Social Security number.

There is no law that prevents businesses from asking for your SSN. And you may be denied service if you don't give the number. If giving your SSN to a business doesn't seem reasonable to you, ask if you can show another form of identification. Or ask if the business can use another number as your customer number.

Remember that some government agencies can require your SSN. These agencies include DMV, welfare offices, and tax agencies. Look for the required "disclosure" form. The form should state if giving the number is required or optional, how it will be used, and the agency's legal authority to ask for it.[1]

⊡ California law limits the public display of Social Security numbers.

A new California law bars many organizations from publicly displaying SSNs.[2]

The law prohibits:

- Printing SSNs on ID cards or badges,
- Printing SSNs on documents mailed to customers, unless the law requires it or the document is a form or application,

- Requiring people to send SSNs over the Internet, unless the connection is secure or the number is encrypted, and
- Requiring people to use an SSN to log onto a web site, unless a password is also used.

The law applies to businesses and other non-governmental entities—for all accounts opened since July 1, 2002.

⊡ Ask your companies to change now.

Businesses may continue their current practices for using SSNs for existing customers, rather than stopping the practices barred by the new law described above—unless a customer requests otherwise in writing. You can ask a company or other non-government organization to treat your SSN as the law requires now. Send a letter that says something like the following: "As a current customer of [name of organization], I am hereby requesting that you comply with the requirements of California Civil Code section 1798.85 related to your use of my Social Security number. I understand that you have 30 days from the receipt of this letter to comply."

IMPORTANT NOTE: Health care and insurance are exceptions. This law does not apply to them until January 2003, for all requirements except the ban on SSNs on ID cards. By July 2005, they must comply with all requirements.

⊡ Getting a new Social Security number is probably not a good idea.

Victims of identity theft sometimes want to change their Social Security number. The Social Security Administration very rarely allows this. In fact, there are drawbacks to changing your number. It could result in losing your credit history, your academic records, and your professional degrees. The absence of any credit history under the new SSN would make it difficult for you to get credit, rent an apartment, or open a bank account.

⊡ Here's where to get more information on Social Security numbers.

Identity Theft: If you think an identity thief is using your SSN, call the Social Security Fraud Hotline at 1-800-269-0271. If you think someone may be using your SSN to work, check your Social Security Personal Earnings and Benefit Statement. You can get a copy by calling 1-800-772-1213, or online at www.ssa.gov/online/ssa-7004.pdf. Also see the Social Security Administration's booklet "When Someone Misuses Your Number," available at www.ssa.gov/pubs/10064.html.

Also see.

What the Numbers Mean: For an explanation of the numbers in SSNs, see "Structure of Social Security Numbers," by Computer Professionals for Social Responsibility, available at www.cpsr.org/cpsr/privacy/ssn/ssn.structure.html.

More on Protecting Your SSN: "Fact Sheet 10: My Social Security Number: How Secure Is It?" by the Privacy Rights Clearinghouse, available at www.privacyrights.org/fs/fs10-ssn.htm.

Recommended Practices: For recommendations on how organizations can protect privacy in their handling of SSNs, see the Office of Privacy Protection's "Recommended Practices for Protecting the Confidentiality of Social Security Numbers," available at www.privacy.ca.gov/recommendations/ssnrecommendations.pdf. See also "Alternatives to Using Social Security Numbers in Large Organizations," from *Privacy Journal*, at www.epic.org/privacy/ssn/alternatives_ssn.html.

[1] The federal Privacy Act of 1974, 5 U.S. Code 552a, is available at www.privacy.ca.gov/laws.htm.
[2] California Civil Code section 1798.85 can be found at www.privacy.ca.gov/laws.htm.

BLANK

Appendix C: Recommendations on Social Security Numbers

BLANK

CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS

Recommended Practices for Protecting the Confidentiality of Social Security Numbers

June 28, 2002

400 R Street, Suite 3080 ¦ Sacramento, CA 94814 ¦ www.privacy.ca.gov

OFFICE OF Privacy Protection

Recommended Practices for Protecting the Confidentiality of Social Security Numbers

Introduction

The Office of Privacy Protection in the California Department of Consumer Affairs has the statutorily mandated purpose of "protecting the privacy of individuals' personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices."[1] The law specifically directs the Office to "make recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers."[2]

In fulfillment of those obligations, the Office of Privacy Protection is publishing these recommended practices for protecting the confidentiality of Social Security numbers. While many of the recommendations might be applied to protect any sensitive personal information, the focus is on Social Security numbers because of the role they have come to play in the marketplace and in identity theft and other forms of fraud.

In developing the recommendations, the Office of Privacy Protection received consultation and advice from an advisory committee made up of representatives of the financial, insurance, health care, retail and information industries and of consumer privacy advocates.[3] The committee members' contributions were very helpful and are greatly appreciated.

Unique Status of the Social Security Number As a Privacy Risk

The Social Security number (SSN) has a unique status as a privacy risk. No other form of personal identification plays such a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential.[4]

Created by the federal government in 1936 to track workers' earnings and eligibility for retirement benefits, the SSN is now used in both the public and private sectors for a myriad of purposes totally unrelated to this original purpose. It is used so widely because the SSN is a unique identifier that does not change, allowing it to serve many record management purposes.[5]

Today SSNs are used as representations of individual identity, as secure passwords, and as the keys for linking multiple records together. The problem is that these uses are incompatible. The widespread use of the SSN as an individual identifier, resulting in its appearance on mailing labels, ID cards and badges, and various publicly displayed

documents, makes it unfit to be a secure password providing access to financial records and other personal information.[6]

The broad use and public exposure of SSNs has been a major contributor to the tremendous growth in recent years in identity theft and other forms of credit fraud. The need to significantly reduce the risks to individuals of the inappropriate disclosure and misuse of SSNs, has in recent years led California and a few other states to take steps to limit their use and display.[7]

California Law on SSN Confidentiality: Civil Code Section 1798.85

The law, which takes effect beginning July 1, 2002 and must be fully effective no later than July 1, 2005, applies to individuals and non-governmental entities. Under the law's provisions, companies may not do any of the following:

- post or publicly display SSNs,
- print SSNs on identification cards or badges;
- require people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted;
- require people to log onto a web site using an SSN without a password.
- print SSNs on anything mailed to a customer unless required by law or the document is a form or application;

The law has a phased-in compliance schedule:

All subject entities but those involved in providing health care or insurance

7/1/02 Must comply with all requirements for new accounts. May continue former practices on existing accounts, but must comply with requirements within 30 days upon written request from customer.

Entities providing health care or insurance

1/1/03 Must comply with all requirements except ban on putting SSNs on identification cards, for individual policyholders

1/1/04 Must comply with all requirements, including identification card requirement, for new individual and group policyholders.

7/1/05 Must comply with all requirements for all individual and group policyholders in existence prior to 1/1/04.

Fair Information Practice Principles

In developing the recommendations, the Office of Privacy Protection looked first to the widely accepted principles that form the basis of most privacy laws in the United States, Canada, Europe and other parts of the world. The Fair Information Practice Principles are openness, collection limitation, purpose specification, use limitation, data quality, individual participation, security and accountability.[8] While they were developed to guide the drafting of national privacy legislation, the principles are also appropriate for organizations to follow in developing their privacy policies and practices. The practices recommended here are all derived from these basic privacy principles.

Recommended Practices for Protecting the Confidentiality of SSNs

The Office of Privacy Protection's recommendations are intended to serve as guidelines to assist organizations in moving towards the goal of aligning their practices with the widely accepted fair information practice principles described below. These recommended practices address, but are not limited to, the provisions of California Civil Code section 1798.85.

The recommendations are relevant for private- and public-sector organizations, and they apply to the handling of all SSNs in the possession of an organization: those of customers, employees and business partners.

1. Reduce the collection of SSNs.
   Fair Information Practice Principles: Collection Limitation, Use Limitation

   - Collect SSNs preferably only where required to do so by federal or state law.
   - When collecting SSNs as allowed, but not required, by law, do so only as reasonably necessary for the proper administration of lawful business activities.
   - If a unique personal identifier is needed, develop your own as a substitute for the SSN.

2. Inform individuals when you request their SSNs.
   Fair Information Practice Principle: Openness, Purpose Specification

   - Whenever you collect SSNs as required or allowed by law, inform the individuals of the purpose of the collection, the intended use, whether the law requires the number to be provided or not, and the consequences of not providing the number.
   - If required by law, notify individuals (customers, employees, business partners, etc) annually of their right to request that you do not post or publicly display their SSN or do any of the other things prohibited in Civil Code Section 1798.85(a).

3. Eliminate public display of SSNs.
   Fair Information Practice Principle: Security

   - Do not put SSNs on documents that are widely seen by others, such as identification cards, badges, time cards, employee rosters, bulletin board postings, and other materials.
   - Do not send documents with SSNs on them through the mail, except on applications or forms or when required by law[9].
   - When sending applications, forms or other documents required by law to carry SSNs through the mail, place the SSN where it will not be revealed by an envelope window. Where possible, leave the SSN field on forms and applications blank and ask the individual to fill it in before returning the form or application.
   - Do not send SSNs by email unless the connection is secure or the SSN is encrypted.
   - Do not require an individual to send his or her SSN over the Internet or by email, unless the connection is secure or the SSN is encrypted.
   - Do not require individuals to use SSNs as passwords or codes for access to Internet web sites or other services.

4. Control access to SSNs.
   Fair Information Practice Principle: Security

   - Limit access to records containing SSNs only to those who need to see the numbers for the performance of their duties.
   - Use logs or electronic audit trails to monitor employees' access to records with SSNs.
   - Protect records containing SSNs, including back-ups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets.
   - Do not store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.
   - Avoid sharing SSNs with other companies or organizations except where required by law.
   - If you do share SSNs with other companies or organizations, including contractors, use written agreements to protect their confidentiality.
     - Prohibit such third parties from re-disclosing SSNs, except as required by law.
     - Require such third parties to use effective security controls on record systems containing SSNs.
     - Hold such third parties accountable for compliance with the restrictions you impose, including monitoring or auditing their practices.
   - If SSNs are disclosed inappropriately and the individuals whose SSNs were disclosed are put at risk of identity theft or other harm, promptly notify the individuals potentially affected.

5. Protect SSNs with security safeguards.
   Fair Information Practice Principle: Security

   - Develop a written security plan for record systems that contain SSNs.
   - Develop written policies for protecting the confidentiality of SSNs, including but not limited to the following:
     - Adopt "clean desk/work area" policy requiring employees to properly secure records containing SSNs.
     - Do not leave voice mail messages containing SSNs and if you must send an SSN by fax, take special measures to ensure confidentiality.
     - Require employees to ask individuals (employees, customers, etc.) for identifiers other than the SSN when looking up records for the individual.
     - Require employees to promptly report any inappropriate disclosure or loss of records containing SSNs to their supervisors or to the organization's privacy officer.
     - When discarding or destroying records in any medium containing SSNs, do so in a way that protects their confidentiality, such as shredding.[10]

6. Make your organization accountable for protecting SSNs.
   Fair Information Practice Principle: Accountability

   - Provide training and written material for employees on their responsibilities in handling SSNs.
     - Conduct training at least annually.
     - Train all new employees, temporary employees and contract employees.
   - Impose discipline on employees for non-compliance with organizational policies and practices for protecting SSNs.
   - Conduct risk assessments and regular audits of record systems containing SSNs.
   - Designate someone in the organization as responsible for ensuring compliance with policies and procedures for protecting SSNs.

Notes

[1] California Business & Professions Code section 350(a).

[2] California Business & Professions Code section 350(c).

[3] The Advisory Committee members were Victoria Allen of the California Credit Union League; Jennie Bretschneider, Legislative Aide to Senator Debra Bowen; James W. Bruner, Jr., of Orrick, Herrington & Sutcliffe; Shelley Curran of Consumers Union; Mari Frank, Esq., privacy consultant; Beth Givens of the Privacy Rights Clearinghouse; Tony Hadley of Experian; Michael Hensley of LexisNexis; Chris Lewis of Providian and the California Chamber of Commerce; Deborah Pierce of Privacy Activism; Rebecca Richards of TRUSTe; Wendy Schmidt of Federated Department Stores and the California Retailers Association; Elaine Torres of Wells Fargo Bank; and Lee Wood of the Association of California Life & Health Insurance Companies.

[4] Mark Rotenberg, Executive Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center, "Testimony and Statement for the Record," Joint Hearing on SSNs and Identity Theft, Subcommittee on Oversight and Investigations, Committee on Financial Services, and Subcommittee on Social Security, Committee on Ways and Means, U. S. House of Representatives, November 8, 2001. Available at www.epic.org/privacy/ssn/testimony_11_08_2001.html .

[5] *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352, May 2002. Available at www.gao.gov.

[6] Chris Hibbert, Computer Professionals for Social Responsibility, "Frequently Asked Questions on SSNs and Privacy," last modified February 16, 2002. Available at www.cpsr.org/cpsr/privacy/ssn/ssn.faq.html.

[7] Arizona and Rhode Island prohibit the display of students' SSNs on the Internet. In Washington, as the result of an April 2000 executive order of the Governor, state agencies have removed SSNs from many documents where their display was determined not to be necessary. Minnesota's Government Data Practices Act classes SSNs as not public information.

[8] The Fair Information Practice Principles were first formulated by the U.S. Department of Health, Education and Welfare in 1973. They may be found in the Organisation for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at http://www1.oecd.org/publications/e-book/9302011E.PDF. The Principles are the following:

- *Openness*: There should be a general policy of openness about the practices and policies with respect to personal information.
- *Collection Limitation*: Personal information should be collected by lawful and fair means and with the knowledge or consent of the subject. Only the information necessary for the stated purpose should be collected.
- *Purpose Specification*: The purpose for collecting personal information should be specified at the time of collection. Further uses should be limited to those purposes.
- *Use Limitation*: Personal information should not be used for purposes other than those specified, except with the consent of the subject or by the authority of law.
- *Data Quality*: Personal information should be accurate, complete, timely and relevant to the purpose for which it is to be used.
- *Individual Participation*: Individuals should have the right to inspect and correct their personal information.
- *Security*: Personal information should be protected by reasonable security safeguards against such risks as unauthorized access, destruction, use, modification, and disclosure.
- *Accountability*: Someone in an organization should be held accountable for compliance with the organization's privacy policy. Regular privacy audits and employee training should be conducted. The principles

[9] See Appendix 1 for a partial list of laws that authorize or mandate the collection and use of SSNs. See Appendix 2 for a list of laws restricting the disclosure of SSNs. Both Appendices will be updated with more comprehensive information

[10] Note that California Civil Code Section 1798.81requires businesses to destroy customer records containing personal information by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable, before discarding them.

Appendix 1: Federal and California Laws That Authorize or Mandate the Collection and Use of Social Security Numbers[1]

Federal Laws

Federal statute	General purpose for collecting or using SSN	Government entity and authorized or required use
Tax Reform Act of 1976 42 U.S.C. 405(c)(2)(c)(i)	General public assistance programs, tax administration, driver's license, motor vehicle registration	Authorizes states to collect and use SSNs in administering any tax, general public assistance, driver's license, or motor vehicle registration law
Food Stamp Act of 1977 7 U.S.C. 2025(e)(1)	Food Stamp Program	Mandates the secretary of agriculture and state agencies to require SSNs for program participation
Deficit Reduction Act of 1984 42 U.S.C. 1320b-7(1)	Eligibility benefits under the Medicaid program	Requires that, as a condition of eligibility for Medicaid benefits, applicants for and recipients of these benefits furnish their SSNs to the state administering program
Housing and Community Development Act of 1987 42 U.S.C. 3543(a)	Eligibility for HUD programs	Authorizes the secretary of the Department of Housing and Urban Development to require applicants and participants in HUD programs to submit their SSNs as a condition of eligibility
Family Support Act of 1988 42 U.S.C. 405(c)(2)(C)(ii)	Issuance of birth certificates	Requires states to obtain parents' SSNs before issuing a birth certificate unless there is good cause for not requiring the number
Technical and Miscellaneous Revenue Act of 1988 42 U.S.C. 405(c)(2)(D)(i)	Blood donation	Authorizes states and political subdivisions to require that blood donors provide their SSNs
Food, Agriculture, Conservation, and Trade Act of 1990 42 U.S.C. 405(c)(2)(C)	Retail and wholesale businesses participation in food stamp program	Authorizes the secretary of agriculture to require the SSNs of officers or owners of retail and wholesale food concerns that accept and redeem food stamps
Omnibus Budget Reconciliation Act of 1990 - 38 U.S.C. 510(c)	Eligibility for Veterans Affairs compensation or pension benefits programs	Requires individuals to provide their SSNs to be eligible for Department of Veterans Affairs' compensation or pension benefits programs
Social Security Independence and Program Improvements Act of 1994 - 42 U.S.C. 405(c)(2)(E)	Eligibility of potential jurors	Authorizes states and political subdivisions of states to use SSNs to determine eligibility of potential jurors
Personal Responsibility and Work Opportunity Reconciliation Act of 1996 - 42 U.S.C. 666(a)(13)	Various license applications; divorce and child support documents; death certificates	Mandates that states have laws in effect that require collection of SSNs on applications for driver's licenses and other licenses; requires placement in the pertinent records of the SSN of the person subject to a divorce decree, child support order, paternity determination; requires SSNs on death certificates; creates national database for child support enforcement purposes

[1] Table taken from "Social Security Numbers: SSNs Are Widely Used by Government and Could Be Better Protected," Statement of Barbara D. Bovbjerg, Director of Education, Workforce, and Income Security Issues, GAO, April 29, 2002,GAO-02-691T. Available at www.gao.gov.

Federal statute	General purpose for collecting or using SSN	Government entity and authorized or required use
Debt Collection Improvement Act of 1996 31 U.S.C. 7701(c)	Persons doing business with a federal agency	Requires those doing business with a federal agency, i.e., lenders in a federal guaranteed loan program; applicants for federal licenses, permits, right-of-ways, grants, or benefit payments; contractors of an agency and others to furnish SSNs to the agency
Higher Education Act Amendments of 1998 20 U.S.C. 1090(a)(7)	Financial assistance	Authorizes the secretary of education to include the SSNs of parents of dependent students on certain financial assistance forms
Internal Revenue Code (various amendments) 26 U.S.C. 6109	Tax returns	Authorizes the commissioner of the Internal Revenue Service to require that taxpayers include their SSNs on tax returns

Appendix 2: Federal and California Laws That Restrict Disclosure of SSNs[2]

Federal Laws

The following federal laws establish a framework for restricting SSN disclosure:

The Freedom of Information Act (FOIA) (5 U.S.C. 552)
This act establishes a presumption that records in the possession of agencies and departments of the executive branch of the federal government are accessible to the people. FOIA, as amended, provides that the public has a right of access to federal agency records, except for those records that are protected from disclosure by nine stated exemptions. One of these exemptions allows the federal government to withhold information about individuals in personnel and medical files and similar files when the disclosure would constitute a clearly unwarranted invasion of personal privacy. According to Department of Justice guidance, agencies should withhold SSNs under this FOIA exemption. This statute does not apply to state and local governments.

The Privacy Act of 1974 (5 U.S.C. 552a)
The act regulates federal government agencies' collection, maintenance, use and disclosure of personal information maintained by agencies in a system of records.[1] The act prohibits the disclosure of any record contained in a system of records unless the disclosure is made on the basis of a written request or prior written consent of the person to whom the records pertains, or is otherwise authorized by law. The act authorizes 12 exceptions under which an agency may disclose information in its records. However, these provisions do not apply to state and local governments, and state law varies widely regarding disclosure of personal information in state government agencies' control. There is one section of the Privacy Act, section 7, that does apply to state and local governments. Section 7 makes it unlawful for federal, state, and local agencies to deny an individual a right or benefit provided by law because of the individual's refusal to disclose his SSN. This provision does not apply (1) where federal law mandates disclosure of individuals' SSNs or (2) where a law existed prior to January 1, 1975 requiring disclosure of SSNs, for purposes of verifying the identity of individuals, to federal, state or local agencies maintaining a system of records existing and operating before that date. Section 7 also requires federal, state and local agencies, when requesting SSNs, to inform the individual (1) whether disclosure is voluntary or mandatory, (2) by what legal authority the SSN is solicited, and (3) what uses will be made of the SSN. The act contains a number of additional provisions that restrict federal agencies' use of personal information. For example, an agency must maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose required by statute or executive order of the president, and the agency must collect information to the greatest extent practicable directly from the individual when the information may result in an adverse determination about an individual's rights, benefits and privileges under federal programs.

The Social Security Act Amendments of 1990 (42 U.S.C. 405(c)(2)(C)(viii))
A provision of the Social Security Act bars disclosure by federal, state and local governments of SSNs collected pursuant to laws enacted on or after October 1, 1990. This provision of the act also contains criminal penalties for "unauthorized willful disclosures" of SSNs; the Department of Justice would determine whether to prosecute a willful disclosure violation. Because the act specifically cites willful disclosures, careless behavior or inadequate safeguards may not be

[2] Taken from *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352, May 2002. Available at www.gao.gov.

subject to criminal prosecution. Moreover, applicability of the provision is further limited in many instances because it only applies to disclosure of SSNs collected in accordance with laws enacted on or after October 1, 1990. For SSNs collected by government entities pursuant to laws enacted before October 1, 1990, this provision does not apply and therefore, would not restrict disclosing the SSN. Finally, because the provision applies to disclosure of SSNs collected pursuant to laws requiring SSNs, it is not clear if the provision also applies to disclosure of SSNs collected without a statutory requirement to do so. This provision applies to federal, state and local governmental agencies; however, the applicability to courts is not clearly spelled out in the law.

California Laws

Confidentiality of Social Security Numbers (CA Civil Code Section 1798.85)

This law, passed in 2001, bars businesses in California from publicly displaying SSNs in specified ways. It takes effect beginning in July 2002 and ending with its application to health care entities by January 2005. The law was passed to help control many of the common uses of SSNs that can expose people to the risk of identity theft. For details, see Confidentiality of Social Security Numbers, Civil Code Section 1798.85.

Appendix D: Selected News Clips

Identity theft is growing, agency says
Head of state Office of Privacy Protection visits county
The head of a new state agency dedicated to preventing identity theft stopped in Marin yesterday to extol the virtues of paper shredders, "opt-out notices" and regular credit reports.
Marin Independent Journal, by Gary Klein - March 27, 2002

Identity theft increases
As identity thefts go, one of the more galling instances occurred to a Folsom woman a week before the April 15 tax deadline.
Sacramento Bee, by Walter Yost – May 2, 2002

State office helps public protect privacy
The state Office of Privacy was created by legislation, SB 129 by Sen. Steve Peace, in response to the escalating crime and reporting of identity theft.
Sacramento Business Journal – May 3, 2002

State to help businesses implement new privacy law
A guide to help businesses comply with a new law to safeguard the privacy of Social Security numbers, which are often used in identity theft, is being issued by the California Department of Consumer Affairs, Office of Privacy Protection.
Silicon Valley/San Jose Business Journal – July 29, 2002

SR Panelists Warn Of Identity Theft Threat
Identity theft experts warned people Saturday to safeguard their personal information or risk its falling into the hands of a growing number of criminals who specialize in living off other people's money.
Santa Rosa Press Democrat, by Jeremy Hay – August 11, 2002

Laguna Woods picked for state anti-theft bid // Citizens group will help neighbors to combat identity theft in a pilot program
Numbers that say "you" – credit card, bank, social security, driver's license, PIN – oh, what damage they can do when found in the wrong hands.
Orange County Register, by Cheryl Walker – October 10, 2002

California is No. 1 in Privacy Protection
When it comes to protecting the privacy rights of citizens, California is number one, according to a ranking published by the "Privacy Journal" in November 2002.
Inside Privacy, by Susan Jayson – January 9, 2003